Developing Cyberspace Competencies for Air Force Professional Military Education

Dr Robert F. Mills
Dr Richard A. Raines
Major Paul D. Williams, PhD

Center for Cyberspace Research
Air Force Institute of Technology

Please direct questions to
robert.mills@afit.edu
937-255-3636 x4527
DSN 785-3636 x4527

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
01 AUG 2007	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Developing Cyberspace Competencies for Air Force Professional Military Education	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Center for Cyberspace Research Air Force Institute of Technology**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**34**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Developing Cyberspace Competencies for Air Force Professional Military Education

1. AF Cyber Command
   1.1. In December, 2005, the USAF added cyberspace as a domain of operations to its mission statement – "fly and fight in air, space and cyberspace". In November, 2006, the CSAF announced the designation of 8th Air Force as the Air Force Cyber Command (AFCYBER) and charged 8AF with developing a plan for organizing, training and equipping a cyber force. Further, the Chief signaled his "intent to redefine airpower" by focusing on integrating USAF capabilities in air, space, and cyberspace.
   1.2. These events necessitate a cultural change that will impact all AF members. All airmen (to include guard, reserve and civilians) must understand the cyberspace domain and how the US uses it to *project national power* and *deliver sovereign options* for the Commander in Chief. Airmen shall embrace cyberspace as a war-fighting domain of operations on par with air, land, sea and space. Cyberspace is a center of gravity and much of our national power depends upon our interconnectedness and technology infrastructure. Superiority in this domain is therefore essential for strategic, operational and tactical operations.
   1.3. In keeping with the SECAF/CSAF intention to redefine airpower, existing curriculum will need refinement, and new content will need to be developed. Cyberspace is a domain of military operations, and we need to begin growing a cyber culture. The challenge is that there is little or no published doctrine, and source materials are limited to high level concept documents and suppositions about what is (and is not) possible in the cyber domain. Nonetheless, we have to start somewhere. To a great extent, we are in the same situation as Mitchell and Douhet when discussing application of airpower.

2. Professional Military Education (PME).
   2.1. PME conveys a broad body of knowledge and develops the habits of mind essential to the military professional's expertise in the art and science of war. PME is how we can help change the Air Force culture, by producing the following:
      2.1.1. Professionals educated in the profession of arms who possess an intuitive approach to joint war fighting built upon individual Service competencies. The aim is to produce graduates prepared to operate at appropriate levels of war in a joint environment and capable of generating quality tactical, operational, and strategic thought from a joint perspective.
      2.1.2. Critical thinkers who view military affairs in the broadest context and are capable of identifying and evaluating likely changes and associated responses affecting the employment of US military forces.
      2.1.3. Professionals who can develop and execute national military strategies that effectively employ the Armed Forces in concert with other instruments of national power to achieve the goals of national security strategy and policy.

2.2. The PME Continuum. The level and depth of study depends on where members are in their careers, as shown in Table 1. The continuum portrays the focus of each educational level in relation to the tactical, operational, and strategic levels of war. USAF education on cyberspace must account for the depth of education needed for each of the Air Force's professional military education schools. The depth will use Bloom's taxonomy, shown in Table 2.

Table 1 - PME Continuum

Officer Force	
Accession	Knowledge
ASBC	Knowledge/Comprehension
SOS	Knowledge/Comprehension
ACSC	Comprehension
AWC	Analysis/Synthesis
Enlisted Force	
Accession	Knowledge
Airman Leadership	Knowledge
NCO	Knowledge/ Comprehension
SNCO	Comprehension

Table 2 - Bloom's Taxonomy of Knowledge

Competence	Skills demonstrated
Knowledge	Observation and recall of information
Comprehension	Understanding information
Application	Use information
Analysis	Seeing patterns, organizing, recognition of hidden meanings
Synthesis	Use old ideas to create new ones, generalize from given facts
Evaluation	Compare and discriminate between ideas, assess value of theories, make choices based on reasoned argument

3. Cyberspace Curriculum Development. There are six general areas of education with respect to cyberspace, as shown in Table 3. These areas must be well-covered to shape the Air Force culture and embrace cyberspace as a domain of operations.

3.1. Modification. In some cases cyberspace/power can be addressed by altering curriculum content to include new cyberspace concepts. It is anticipated that this content can be simply modified to include the handling of cyberspace as a domain of operations. Coverage at this level should be fairly high, indicating the

importance of cyberspace to our own interests and as a mechanism to project national power.

3.2. New Content. As noted above, the newness of cyberspace and cyber concepts limits what can currently be developed. However, emphasis at this point should be on changing the AF culture. This is a long term process and has two facets. First, we must educate members upon their entry into the Air Force on fundamental concepts, regardless of their specific career field. Second, we have to provide education for our more seasoned existing force, bringing them up to a baseline understanding of cyberspace and cyber operational capabilities. The table below outlines six areas of instruction regarding cyberspace and cyber operations to be included into the existing PME curricula.

Table 3 - Cyberspace Competency Areas

Nature & characteristics of the domain
• Military domain of operations – where we conduct operations to achieve effects • Cyberspace is an operational area consisting of the entire electromagnetic spectrum (EMS) and electronic systems • Comparison / contrast with other domains of air, land, space, and sea • Cyberspace domain transcends all other domains
Capabilities
• The AF has a broad range of capabilities that operate in the cyberspace domain, including network warfare (NW) and electronic warfare (EW) and Influence operations • Capabilities include offense, defense, and support • Synergistic application of cyber and non-cyber capabilities in other domains
Functions
• AF functions are performed to achieve effects in support of national security objectives • Strategic attack, cyberspace control, cyberspace interdiction, etc. • Functions include Intelligence, Surveillance and Reconnaissance, Information Operations, Navigation and Positioning, Command and Control, and Weather Services (+ counter space)
Integration & interrelationships
• Interrelationship between air, space and cyberspace forces is complex. • Cyberspace capabilities can support & enhance activities in other domains • Activities in other domains can support & enhance cyberspace operations • Examples: jamming adversary communication and radar systems to support air, ground and sea operations; using kinetic weapons to achieve cyber effects

- Integrating these capabilities at the operational level is complex
- Detailed integration between services/components and other governmental (including law enforcement) agencies is required for offensive and defensive operations

Employment of Cyberpower

- Cyberpower theory and doctrine
- Tracing from strategy/policy to theory to operational tasks
- Employing/integrating cyber into the joint planning process
- Instruments of national power – cyberspace increasing the importance of information
- Organizing for effective employment of cyberpower
- Tenets / principles of air/space/cyberpower
- Control / dominate of all three domains—whoever controls cyberspace can control the other domains
- 24 x 7 x 365 cyber effects at all levels of war

Law, policy & ethics

- US laws (criminal, administrative, and civil)
- Restrictions on what military forces can do, especially in the homeland (Privacy rights, Posse Comitatus, Intelligence Oversight, Title 10/50)
- International Laws affecting electronic communications
- Military Law (UCMJ, Nat'l Security Act, Foreign Intel Surveillance Act, etc.)
- Law of Armed Conflict (jus ad bellum, jus in bello, principles of discrimination & proportionality, targeting, combatants)
- Potential use of cyber capabilities as weapons of mass destruction/effects

4. Table 4 demonstrates an alternate view of Cyber Warfare. Since the Eighth Air Force Concept of Cyber Warfare has been published, we recommend that the same material suggested above should still be covered but in the same framework as the CONOPS. Utilizing this framework would follow a proper Strategic Communications approach in which the entire Air Force is being taught to think about cyberspace and cyber operations the same way. This would also allow for faster culture changes since everyone would be on the same page and speaking the same language.
   4.1. We've provided the following table as a suggested set of competencies, but have expanded on the original set for the remainder of this document. Since the material is basically the same, simply organized differently, this should allow for a relatively simple conversion between the two versions once a proper way forward is determined.
   4.2. The content in this table is drawn from the Concept of Cyber Warfare[1] document and in some cases is directly copied from that source.

Table 4 – Alternative Cyberspace Competency Areas

Cyber Warfare Fundamentals

- Cyberspace is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures
- Cyberspace exists across the other physical domains of air, land, sea, and space and can facilitate contact between the cognitive processes and the physical domains
- Increased national and military dependence on cyberspace creates a national vulnerability
- The low-cost, speed, and anonymity of actions within cyberspace allows militarily inferior adversaries to cause potentially catastrophic affects with a country highly dependent on technology
- United States' *National Strategy to Secure Cyberspace* and Air Force cyberspace objectives
- First priority to ensure friendly use of cyberspace while denying that same use to the adversary
- Three categories of war-fighting operations in cyberspace (ensuring operational freedom of action, delivering cross domain effects, supporting civil operations)
- Cyber superiority is the freedom to operate in cyberspace while denying that ability to an adversary
- Operations in all other domains are heavily dependent on unrestricted access to cyberspace
- Cyberspace links the physical domains with a forces decision processes
- Cyber capabilities can be used to defend and protect critical civilian infrastructure, as well as support the defense industrial base in protecting sensitive information

Operations in Cyberspace

- Cyber operations can be conducted at any level of war and across the entire spectrum of conflict in support of global and theater objectives
- Cyberspace capabilities include counter-cyber operations, information operations, intelligence, surveillance and reconnaissance, and combat support
- Counter-cyber Operations is an Air Force function, the objective of which is cyber superiority
- Involves those operations conducted to ensure friendly freedom of action within and to exploit cyberspace while denying the same to our adversaries when required.
- Conducted by air, space, land, sea, cyber, or special operations forces (SOF)
- Operations include both Offensive Counter-cyber (OCC) and Defensive Counter-cyber (DCC)

- Cyber capabilities can be used to achieve effects in other domains and conventional attack capabilities can achieve desired effects in cyberspace
- Cyber Warfare and Information Operations are separate entities, however, Information Operations can and do take place within cyberspace
- Near and long-term challenges are the development of cyberspace infrastructure, systems, and force
- Cyber infrastructure includes everything operating in, creating access to, and containing cyberspace
    - Examples: weapons, sensors, tools, facilities, software, networks, hardware, ranges
- Current infrastructure is largely commercial; must assess and quantify risks associated
- Infrastructures must be made to be survivable (secure, protected, redundant, etc.) and standardized
- Current acquisition process is not suitable for cyber systems; must create a process to allow rapid development and response to emerging threats (may increase risks associated with new systems)
- AF must develop a professional force of cyber leaders and cyber warriors who understand how to operate in cyberspace and integrate cyber operations with other capabilities to deliver desired effects

Command and Control

- There are many national players in cyber operations (NSA, DIA, DHS, CIA, FBI, other services, etc.)
- Global coordination required since cyber assets can be national and theater level assets at the same time and specific portions of cyberspace can be affected by multiple assets at the same time
- An interoperable C2 structure is needed to enable deconfliction and visibility of all cyber taskings
- Plan should address how to integrate, coordinate, and deconflict the use of cyberspace with the host nation or other US agencies for non-military operations as well
- JFC must be responsible for protection and defending friendly cyberspace

Law, Policy, and Ethics

- US laws (criminal, administrative, and civil)
- Restrictions on what military forces can do, especially in the homeland (Privacy rights, Posse Comitatus, Intelligence Oversight, Title 10/50)
- International Laws affecting electronic communications
- Military Law (UCMJ, Nat'l Security Act, Foreign Intel Surveillance Act, etc.)
- Law of Armed Conflict (jus ad bellum, jus in bello, principles of discrimination & proportionality, targeting, combatants)
- Potential use of cyber capabilities as weapons of mass destruction/effects

5. Cyber Learning Areas and Objectives. The following sections provide guidelines for adding cyberspace concepts into the Air Force PME schools. Each school will need to assess their own curriculum and determine how best to develop/modify their curriculum.

Officer PME

Table 5 - Officer Accession (Appreciate)

Area	Concepts
Nature & characteristics of the domain	• Cyberspace domain is an operational domain consisting of the entire electromagnetic spectrum (EMS), networks, and electronic systems • Comparison / contrast with other domains of air, land, space, and sea • Cyberspace domain transcends all other domains
Capabilities	• The AF has a broad range of capabilities that operate in cyberspace, such as network capabilities and electronic warfare • Capabilities include offense, defense, and support • Capabilities are planned and employed in conjunction with operations in other domains to achieve national security objectives
Functions	• AF functions (e.g. Intelligence, Surveillance and Reconnaissance, Information Operations, Command and Control, etc.) are performed to achieve effects in support of national security objectives • Strategic attack, cyberspace control, cyberspace interdiction, etc.
Integration & interrelationships	• Interrelationship between air, space and cyberspace forces is complex. • Cyberspace capabilities can support & enhance activities in other domains • Activities in other domains can support & enhance cyberspace operations • Cyberspace is crucial to effectiveness in other domains • Integrating these forces at the operational level is complex • Distinguish between cyberspace and information operations—AF position is that cyber is **not** just a rehash of IO, rather IO attains effects in cyberspace • Military Services' primary roles, missions and organizations. This should already exist at a conceptual level. Cyber should be addressed as a third mission area for the USAF, and content will discuss at a conceptual

	level how cyber forces are organized, trained and equipped for cyber operations. Also describe how these forces are presented to the combatant commanders.
Employment of cyberpower	• Organizing for effective employment of cyberpower • Primary missions and responsibilities of the combatant commands • Instruments of national power – cyberspace increasing the importance of information • Effective application of air, space and cyberpower: compress kill chain, secure C2, cross-domain dominance) • Tenets / principles of air, space, and cyberspace • 24 x 7 x 365 cyber effects at all levels of war
Law, policy & ethics	• There are restrictions on what military forces can do, especially in the homeland (Posse Comitatus, Intelligent Oversight, Title 10/50) • Law of Armed Conflict (jus ad bellum, jus in bello, principles of discrimination & proportionality, targeting, combatants) • Appreciate cyberspace's use as a potential WMD/E

6. Squadron Officer College (SOC):
   6.1. Mission: *Develop twenty-first century Airmen who can advocate what air, space, and cyberspace power brings to the fight, value team achievement over individual success, and value their role in the profession of arms.*[4]

7. Specific to Air & Space Basic Course (ASBC):
   7.1. Mission: *To inspire new USAF officers to comprehend their roles as Airmen who understand and live by USAF core values, can articulate and advocate what air, space, and cyberspace power brings to the fight, and are dedicated as warriors in the world's most respected air, space, and cyberspace force.*[4]
   7.2. Goals[4]:
      7.2.1. Embrace the profession of arms by applying the Air Force core values with the heart, mind, and body of an air, space, and cyberspace warrior.
      7.2.2. Value the expeditionary air, space, and cyberspace force as a team, and the role of Air Force officers in leading within this team.
   7.3. Comprehend air, space, and information operations as the primary means for effectively employing air, space, and cyberspace power as a part of the joint war-fighting team.
   7.4. Comprehend Air Force history, doctrine, and distinctive capabilities as the foundation or the effective employment of air, space, and cyberspace power.

Table 6 - ASBC (Knowledge/Comprehension)

Area	Concepts
Nature & characteristics of the domain	• Definition of a "military domain of operations" • Cyberspace as an operational domain—i.e., a place where we conduct operations to achieve effects and exert will over the adversary • Compare / contrast with other domains of air, land, space, and sea • Cyberspace domain is an operational area consisting of the entire electromagnetic spectrum (EMS), networks, and electronic systems • Characteristics, physics, boundaries, etc. • Cyberspace domain transcends all other domains • Know the organization for national security and how defense organizations fit into the overall structure (Modification)
Capabilities	• The AF has a broad range of capabilities that operate in cyberspace, such as network capabilities and electronic warfare, and Influence operations • Capabilities include offense, defense, and support • Capabilities are planned and employed in conjunction with operations in other domains to achieve national security objectives • Understand fundamentals of information operations (This should exist per OPMEP requirements. However, the Air Force position is that *cyber operations* is not just a new term for information operations. Cyberspace is a domain of operations in which we achieve effects. Information operations may be performed in all of the domains to include cyberspace. With this in mind, we will need to modify our curriculum to distinguish cyberspace as a domain from information operations which are conducted in a domain.)
Functions	• AF functions (Intelligence, Surveillance and Reconnaissance, Information Operations, Command and Control, etc.) are performed to achieve effects in support of national security objectives • Strategic attack, cyberspace control, cyberspace interdiction, etc. • Functions include Intelligence, Surveillance and Reconnaissance, Information Operations, Command and Control, Counterspace, etc. • Students will know how the functions support, integrate with, and depend on other functions

Integration & interrelationships	• Cyberspace capabilities can support & enhance activities in other domains • Activities in other domains can support & enhance cyberspace operations • Cyberspace is crucial to effectiveness in other domains • Integrating these forces at the operational level is complex • Distinguish between cyberspace and information operations—AF position is that cyber is **not** just a rehash of IO, rather IO attains effects in cyberspace • Interrelationship between air, space and cyberspace forces is complex. • Examples: jamming adversary communication and radar systems to support air, ground and sea operations; using kinetic weapons to achieve cyber effects
Employment of cyberpower	• Primary missions and responsibilities of the combatant commands • Organizing for effective employment of cyberpower • Know the effects that can be achieved with information operations and the implications for tactical operations. • Instruments of national power – cyberspace increasing the importance of information • Effective application of air, space and cyberpower: compress kill chain, secure C2, cross-domain dominance) • Tenets / principles of air, space, and cyberspace • 24 x 7 x 365 cyber effects at all levels of war • Know that first priority is to control / dominate all three domains—whoever controls cyberspace generally controls the air, the land, the sea, and space • Military Services' primary roles, missions and organizations (This should already exist at a conceptual level. Cyber should be addressed as a third mission area for the USAF, and content will discuss at a conceptual level how cyber forces are organized, trained and equipped for cyber operations. Also describe how these forces are presented to the combatant commanders.) • Know the capabilities of other Services' weapon systems pertinent to the Service host-school systems and the synergistic effect gained from effective use of their joint capabilities
Law, policy & ethics	• Recognize how factors such as geopolitics, culture and religion play in shaping planning and execution of joint force operations. Understand the impact of cyberspace and international communications infrastructure

	• US laws (criminal, administrative, and civil) • Restrictions on what military forces can do, especially in the homeland (Posse Comitatus, Intelligent Oversight, Title 10/50) • Rules of Engagement (ROE) and tailored response options • International Laws affecting electronic communications • Military Law (UCMJ, Nat'l Security Act, Foreign Intel Surveillance Act, etc.) • Law of Armed Conflict (jus ad bellum, jus in bello, principles of discrimination & proportionality, targeting, combatants) • Understand cyberspace's use as a potential WMD/E

8. Specific to Squadron Officer School (SOS):
   8.1. Mission: *Develop dynamic Airmen ready to lead air, space, and **cyberspace** power in an expeditionary war-fighting environment.*[4]
   8.2. Goals[4]:
      8.2.1. Broadening commitment to the concept of officership, core values, and the unique role of the Air Force officer in the profession of arms
      8.2.2. Valuing the distinctive capabilities of air, space, and **cyberspace** power as guided by Air Force doctrine and apply those principles to current and future war-fighting scenarios
      8.2.3. Strengthening leadership and followership skills by building effective, cohesive teams that can adapt successfully to accomplish challenging goals
      8.2.4. Applying sound problem-solving, management, and communication practices to operate successfully in an expeditionary war-fighting environment.

Table 7 - SOS (Knowledge/Comprehension)

Area	**Concepts**
Nature & characteristics of the domain	• Definition of a "military domain of operations" • Cyberspace as an operational domain—i.e., a place where we conduct operations to achieve effects and exert will over the adversary • Compare/ contrast with other domains of air, land, space, and sea • Cyberspace domain is an operational area consisting of the entire electromagnetic spectrum (EMS), networks, and electronic systems • Characteristics, physics, boundaries, etc. • Cyberspace domain transcends all other domains • Know the organization for national security and how defense organizations fit into the overall structure

Capabilities	• The AF has a broad range of capabilities that operate in cyberspace, such as network capabilities and electronic warfare and Influence operations • Capabilities include offense, defense, and support • Capabilities are planned and employed in conjunction with operations in other domains to achieve national security objectives • Understand fundamentals of information operations (This content should exist per OPMEP requirements. However, the Air Force position is that *cyber operations* is not just a new term for information operations. Cyberspace is a domain of operations in which we achieve effects. Information operations may be performed in all of the domains to include cyberspace. With this in mind, we will need to modify our curriculum to distinguish cyberspace as a domain from information operations which are conducted in a domain.)
Functions	• AF functions (e.g. Intelligence, Surveillance and Reconnaissance, Information Operations, Command and Control, etc.) are performed to achieve effects in support of national security objectives • Strategic attack, cyberspace control, cyberspace interdiction, etc. • Functions include Intelligence, Surveillance and Reconnaissance, Information Operations, Command and Control, etc. • Students will know how the functions support, integrate with, and depend on other functions
Integration & interrelationships	• Cyberspace capabilities can support & enhance activities in other domains • Activities in other domains can support & enhance cyberspace operations • Cyberspace is crucial to effectiveness in other domains • Integrating these forces at the operational level is complex • Distinguish between cyberspace and information operations—AF position is that cyber is **not** just a rehash of IO, rather IO attains effects in cyberspace • Interrelationship between air, space and cyberspace forces is complex. • Examples: jamming adversary communication and radar systems to support air, ground and sea operations; using kinetic weapons to achieve cyber effects
Employment of	• Primary missions and responsibilities of the combatant

cyberpower	commands • Organizing for effective employment of cyberpower • Know the effects that can be achieved with information operations and the implications for tactical operations • Instruments of national power – cyberspace increasing the importance of information • Effective application of air, space and cyberspace: compress kill chain, secure C2, cross-domain dominance) • Tenets / principles of air, space, and cyberspace • 24 x 7 x 365 cyber effects at all levels of war • Know that first priority is to control / dominate all three domains—whoever controls cyberspace generally controls the air, the land, the sea, and space • Military Services' primary roles, missions and organizations (This should already exist at a conceptual level. Cyber should be addressed as a third mission area for the USAF, and content will discuss at a conceptual level how cyber forces are organized, trained and equipped for cyber operations. Also describe how these forces are presented to the combatant commanders.) • Know the capabilities of other Services' weapon systems pertinent to the Service host-school systems and the synergistic effect gained from effective use of their joint capabilities
Law, policy & ethics	• Recognize how factors such as geopolitics, culture and religion play in shaping planning and execution of joint force operations • Understand the impact of cyberspace and international communications infrastructure • US laws (criminal, administrative, and civil) • Restrictions on what military forces can do, especially in the homeland (Posse Comitatus, Intelligent Oversight, Title 10/50) • Rules of Engagement (ROE) and tailored response options • International Laws affecting electronic communications • Military Law (UCMJ, Nat'l Security Act, Foreign Intel Surveillance Act, etc.) • Law of Armed Conflict (jus ad bellum, jus in bello, principles of discrimination & proportionality, targeting, combatants) • Understand cyberspace's use as a potential WMD/E

9. Air Command and Staff College (ACSC):
   9.1. Mission: *To our students . . . inspire critically thinking Airmen to lead Air and Space forces in joint/combined operations. To our faculty and staff . . . provide an intellectually stimulating environment that attracts, develops, and rewards the finest team of educator-leaders possible.*[4]
   9.2. Goals[4]:
      9.2.1. ACSC graduates are well educated in the profession of arms with emphasis on the use of air and space power in joint campaign planning and the operational art of war. The ACSC Curriculum
         9.2.1.1. Facilitates the air- and space-minded thinking of students
         9.2.1.2. Develops and enhances abilities for higher-level command and staff responsibilities
         9.2.1.3. Enhances students' abilities to think critically about operational air and space concepts in a dynamic international environment
         9.2.1.4. Broadens students' understanding of the nature of conflict and current and future threats to the United States and its allies
         9.2.1.5. Develops and enhances students' abilities to plan and execute the joint campaign planning process and air and space operations to support the joint force commander

Table 8 – ACSC (Comprehension)

Area	**Concepts**
Nature & characteristics of the domain	• Comprehend concept of "military domain of operations" • Cyberspace as an operational domain—i.e., a place where we conduct operations to achieve effects and exert will over the adversary • Compare / contrast cyber with other domains of air, land, space, and sea. Comprehend nature of military operations in these domains. • Cyberspace domain is an operational area consisting of the entire electromagnetic spectrum (EMS), networks, and electronic systems • Characteristics, physics, boundaries, etc. • Comprehend how cyberspace domain transcends all other domains
Capabilities	• Comprehend the capabilities and limitations of US military forces to conduct the full range of military operations against the capabilities of 21st century adversaries, to include cyberspace • Understand fundamentals of information operations (This content should exist per OPMEP requirements. AF believes *cyber operations* is not just a new term for information operations. Cyberspace is a domain of operations in which we achieve effects. Information operations may be performed in all of the domains to

	include cyberspace. With this in mind, we will need to modify our curriculum to distinguish cyberspace as a domain from information operations which are conducted in a domain.) • Understand the AF has a broad range of capabilities that operate in the EMS, such as network capabilities and electronic warfare • Capabilities include offense, defense, and support • Capabilities are planned and employed in conjunction with operations in other domains to achieve national security objectives
Functions	• AF functions (e.g. Intelligence, Surveillance and Reconnaissance, Information Operations, Command and Control, Weather Services, etc.) are performed to achieve effects in support of national security objectives • Strategic attack, cyberspace control, cyberspace interdiction, etc. • Comprehend how these functions support, integrate with, and depend on other functions
Integration & interrelationships	• Cyberspace capabilities can support & enhance activities in other domains • Activities in other domains can support & enhance cyberspace operations • Integrating these forces at the operational level is complex • Distinguish between cyberspace and information operations—AF position is that cyber is **not** just a rehash of IO, rather IO attains effects in cyberspace • Comprehend the complexity of the interrelationship between air, space and cyberspace forces • Comprehend how cyberspace capabilities can support & enhance activities in other domains • Examples: jamming adversary communication and radar systems to support air, ground and sea operations; using kinetic weapons to achieve cyber effects
Employment of cyberpower	• Comprehend the relationships among national objectives, military objectives and conflict termination; understand how cyberpower can be employed to achieve objectives • Comprehend the relationships among the strategic, operational and tactical levels of war and how cyberpower crosses them • Comprehend the relationships between all elements of national power (diplomatic, information, military, economic – consider other factors such as intelligence,

	finance, and law enforcement) • Comprehend importance of interagency and multinational coordination in planning and conducting cyber operations, to include homeland security • Comprehend the effect of time, coordination, policy changes and political development on the planning process for cyber operations • Comprehend how cyber operations are incorporated into both adaptive and crisis-action planning processes at the operational and JTF and JFACC/JAOC levels • Comprehend how C2 and battlespace awareness apply at the operational level of war and how they support operations conducted by a networked force • Comprehend how increased reliance on information technology throughout the range of military operations creates opportunities and vulnerabilities • Comprehend how complexity of cyberspace creates opportunities for asymmetric attacks against the US and its allies • Evaluate the national military strategy, especially with respect to the changing nature of warfare and global interconnectivity • Analyze joint operational art and emerging joint operational concepts with regards to cyber operations • Appraise processes for coordinating US military plans and actions effectively with forces from other countries and with interagency and non-governmental organizations to include homeland security and defense • Analyze how cyber and information operations are integrated to support the national military and national security strategies and the interagency process • Analyze how cyber and information operations apply at the operational and strategic levels of war and how they support the operations of a networked force • Analyze the principles, capabilities and limitations of cyber operations across the range of military operations and plans – to include pre- and post-conflict operations • Analyze the use of cyber operations to achieve desired effects across the spectrum of national security threats • Comprehend primary missions and responsibilities of the combatant commands • Comprehend how theory and principles of war pertain to the operational level of war • Comprehend considerations for employing joint and multinational forces at the operational level of war

	• Comprehend the organizational framework within which joint forces are created, employed and sustained • Military Services' primary roles, missions and organizations (Cyber should be addressed as a third mission area for the USAF, and content will discuss at a conceptual level how cyber forces are organized, trained and equipped for cyber operations. Also describe how these forces are presented to the combatant commanders.) • Understand capabilities of other Services' and the synergistic effect gained from effective use of their joint capabilities • Organizing for effective employment of air, space, and cyberspace • Effective application of air, space and cyberspace: compress kill chain, secure C2, cross-domain dominance) • Tenets / principles of air, space, and cyberspace • 24 x 7 x 365 cyber effects at all levels of war • Comprehend that first priority is to control / dominate all domains—whoever controls cyberspace generally controls the air, the land, the sea, and space
Law, policy & ethics	• Comprehend how joint force command relationships and directive authority for logistics support joint warfighting capabilities • Recognize how factors such as geopolitics, culture and religion play in shaping planning and execution of joint force operations, and understand the impact of cyberspace and international communications infrastructure on these factors • Comprehend restrictions on what military forces can do, especially in the homeland (Posse Comitatus, Intelligent Oversight, Title 10/50) • US laws (criminal, administrative, and civil) • Rules of Engagement (ROE) and tailored response options • International Laws affecting electronic communications • Military Law (UCMJ, Nat'l Security Act, Foreign Intel Surveillance Act, etc.) • Law of Armed Conflict (jus ad bellum, jus in bello, principles of discrimination & proportionality, targeting, combatants) • Understand cyberspace's use as a potential WMD/E

10. Air War College (AWC):
    10.1. Mission: Develop and support senior leaders through education, research, and information programs focused on strategic and institutional leadership, joint and multinational war-fighting, multi-agency international security operations, air and space force development, and national security planning.[4]
    10.2. Goals:
        10.2.1. To be prepared for the responsibilities of strategic leadership in joint, interagency, and multinational environments, AWC graduates will demonstrate mastery in the following ways:
            10.2.1.1. Analyze, synthesize, articulate, apply, and/or evaluate concepts and learning area objectives embodied in CJCSI 1800.10C, *Officer Professional Military Education Program*, for senior-level colleges
            10.2.1.2. Evaluate current national military strategy in the context of historical and contemporary applications of foundational principles of strategy and security policy
            10.2.1.3. Evaluate the role played by fundamental elements of strategy in shaping the outcomes and methods of contemporary campaigns and in joint, interagency, and multinational war-fighting
            10.2.1.4. Develop critical analysis and creative thinking skills, self-awareness, cross-cultural communications and negotiation skills, and decision-making skills in a vulnerable, uncertain, complex, and ambiguous environment
            10.2.1.5. Evaluate the leadership characteristics and capabilities needed by strategic leaders for ethically leading the institution in a joint, interagency and multinational environment
            10.2.1.6. Assess the context and content of the processes used in developing US security strategy policy and the planning, development, and acquisition of military forces to support the policy
            10.2.1.7. Assess overarching social, cultural, religious, political, and economic currents that influence global, regional, and national security conditions; and the US policy responses to those conditions using a diplomatic, informational, military, economic-culture model
            10.2.1.8. Assess the role and impact of civilian-military relations and the bureaucratic political impacts within the national policy-maker environment on policy development and execution with a special emphasis on this relationship within the national capitol region
            10.2.1.9. Examine the roles nations and non-state actors play in addressing key issues that shape the global environment
            10.2.1.10. Identify growing and emerging security concerns beyond the military capabilities of state and non-state actors
            10.2.1.11. Provide the tools needed to develop, deploy, employ, and control joint forces across the spectrum of conflict
            10.2.1.12. Evaluate the strategic implications of emerging war-fighting concepts (sister service, Global Strategic Operations, logistics, and Special Operations), planning for and evaluation of future threats that

are asymmetric to the US experience and expectations, and examination of one's efforts from an opposing perspective; and

10.2.1.13. Assess emerging friction points within and between joint and service operational concepts

Table 9 – AWC (Application)

Area	**Concepts**
Nature & characteristics of the domain	• Comprehend concept of "military domain of operations" • Cyberspace as an operational domain—i.e., a place where we conduct operations to achieve effects and exert will over the adversary • Compare / contrast cyber with other domains of air, land, space, and sea; analyze nature of military operations in these domains • Analyze how cyberspace domain transcends all other domains
Capabilities	• Analyze capabilities and limitations of US military forces to conduct the full range of military operations against the capabilities of 21st century adversaries, to include cyberspace • Apply fundamentals of cyber and information operations (This content should exist per OPMEP requirements. AF believes *cyber operations* is not just a new term for information operations. Cyberspace is a domain of operations in which we achieve effects. Information operations may be performed in all of the domains to include cyberspace. With this in mind, we will need to modify our curriculum to distinguish cyberspace as a domain from information operations which are conducted in a domain.) • Advocate for and defend capabilities in cyberspace such as network capabilities and electronic warfare
Functions	• Analyze how cyberspace functions are performed to achieve effects in support of national security objectives • Analyze how these functions support, integrate with, and depend on other functions
Integration & interrelationships	• Synthesize and evaluate how cyberspace capabilities can support and be supported by activities in other domains • Integrate air, space, and cyberspace forces and capabilities at the operational level • Analyze and evaluate integration of cyber and information operations with conventional operations
Employment of cyberpower	• Analyze the relationships among national objectives, military objectives and conflict termination; understand

	how cyberpower can be employed to achieve objectives • Analyze the relationships among the strategic, operational and tactical levels of war and how cyberpower crosses them • Analyze the relationships between all elements of national power (diplomatic, information, military, economic – consider other factors such as intelligence, finance, and law enforcement) • Analyze importance of interagency and multinational coordination in planning and conducting cyber operations, to include homeland security • Analyze the effect of time, coordination, policy changes and political development on the planning process for cyber operations • Synthesize and evaluate how cyber operations are incorporated into both adaptive and crisis-action planning processes at the operational and JTF levels • Analyze how C2 and battlespace awareness apply at the operational level of war and how they support operations conducted by a networked force • Analyze how increased reliance on information technology throughout the range of military operations creates opportunities and vulnerabilities • Evaluate the national military strategy, especially with respect to the changing nature of warfare and global interconnectivity • Analyze joint operational art and emerging joint operational concepts with regards to cyber operations • Appraise processes for coordinating US military plans and actions effectively with forces from other countries and with interagency and non-governmental organizations to include homeland security and defense • Analyze how cyber and information operations are integrated to support the national military and national security strategies and the interagency process • Analyze how cyber and information operations apply at the operational and strategic levels of war and how they support the operations of a networked force • Analyze the principles, capabilities and limitations of cyber operations across the range of military operations and plans – to include pre- and post-conflict operations • Analyze the integration of all instruments of national power in achieving strategic objectives, with a focus on the employment of the military instrument of national power both as a supported instrument and as a supporting instrument of national power

	• Evaluate the national military strategy, especially with respect the changing nature of warfare • Evaluate the principles of joint warfare, joint military doctrine and emerging concepts to joint, unified, interagency and multinational operations, in peace and war • Evaluate how joint, unified, and multinational campaigns and operations support national objectives and relate to the national strategic, national military strategic, theater strategic and operational levels in war • Analyze the integration of joint, interagency, and multinational capabilities across the range of military operations and plans - both in preparation and execution phases - and evaluate its success in achieving the desired effects • Comprehend the attributes of the future joint force and how this force will organize, plan, prepare and conduct operations • Analyze how information operations are integrated to support the national military and national security strategies and the interagency process • Analyze Military Services' primary roles, missions and organizations (Cyber should be addressed as a third mission area for the USAF, and content will discuss at a conceptual level how cyber forces are organized, trained and equipped for cyber operations. Also describe how these forces are presented to the combatant commanders.) • Understand capabilities of other Services' and the synergistic effect gained from effective use of their joint capabilities
Law, policy & ethics	• Analyze joint force command relationships and directive authority • Analyze how factors such as geopolitics, culture and religion play in shaping planning and execution of joint force operations, including the impact of cyberspace and international communications infrastructure • Evaluate restrictions on what military forces can do, especially in the homeland (Posse Comitatus, Intelligent Oversight, Title 10/50) • Develop and evaluate Rules of Engagement (ROE) and tailored response options in light of US, international, and military law • Synthesize and evaluate targeting recommendations in light of Law of Armed Conflict considerations

	• Analyze cyberspace's use as a potential WMD/E

Enlisted PME

11. Enlisted PME attempts to broaden enlisted members' perspectives and increase their knowledge of military studies, communicative skills, leadership, QAF principles, concepts, and supervision. It prepares them to assume more responsibility.
    11.1. There are several major differences between the focus of EPME and OPME. While both curriculums spend a large portion of their time on developing leadership and management skills, EPME still focuses on a lower level of leadership/supervision. Along those same lines, a large portion of the PME for the enlisted force, specifically for grades E-1 through E-6, focuses on the tactical level of war. Officers, on the other hand, begin the shift from the tactical to operational level at the O-3 level and then focus on operational levels of war as an O-4. The strategic level of war does not enter the enlisted PME until an airman reaches E-9, where officers begin working on the strategic level at O-5 and continue at that level for the rest of their career. Additionally, early EPME focuses on service and job specific topics, where as OPME starts working towards joint operations even as early as pre-commissioning education. For a graphical depiction of these differences, see sections "A-A-A-1" in both CJCSI 1800.01C[13] and CJCSI 1805.01[14].

Table 10 - Enlisted Accession (Appreciate)

Area	Concepts (Appreciate)
Nature & characteristics of the domain	• Cyberspace domain is an operational domain consisting of the entire electromagnetic spectrum (EMS) and electronic systems • Cyberspace domain transcends all other domains
Capabilities	• The AF has a broad range of capabilities that operate in cyberspace, such as network capabilities and electronic warfare • Capabilities include offense, defense, and support
Functions	• AF functions are performed to achieve effects in support of national security objectives • Strategic attack, cyberspace control, cyberspace interdiction, etc. • Functions include Intelligence, Surveillance and Reconnaissance, Information Operations, Command and Control, etc.
Integration & interrelationships	• Interrelationship between air, space and cyberspace forces is complex. • Distinguish between cyberspace and information

	operations—AF position is that cyber is **not** just a rehash of IO • Military Services' primary roles, missions and organizations. This should already exist at a conceptual level. Cyber should be addressed as a third mission area for the USAF, and content will discuss at a conceptual level how cyber forces are organized, trained and equipped for cyber operations. Also describe how these forces are presented to the combatant commanders.
Employment of cyber power	• Instruments of national power – cyberspace increasing the importance of information • Tenets / principles of air, space, and cyber power • 24 x 7 x 365 cyber effects at all levels of war
Law, policy & ethics	• There are restrictions on what military forces can do, especially in the homeland (Posse Comitatus, Intelligent Oversight, Title 10/50) • Law of Armed Conflict (jus ad bellum, jus in bello, principles of discrimination & proportionality, targeting, combatants)

12. Airman Leadership School (ALS):
    12.1. The ALS prepares senior airmen (SrA) to assume supervisory duties. This entry-level enlisted PME program is available to SrA after reaching 48 months of TAFMS or after being selected for promotion to SSgt. The 4-week course offers instruction and practice in leadership and followership, written and oral communicative skills, and profession of arms. Students learn to appreciate their role as military supervisors and how they contribute to the overall goals and mission of the Air Force. (Note: SrA must complete ALS to assume the rank of SSgt.). [5]
        12.1.1. Mission: *Prepare senior Airmen to be professional, war-fighting Airmen who can supervise and lead Air Force work teams to support the employment of air, space, and **cyberspace** power.*[4]
        12.1.2. Goal: Provide senior Airmen an opportunity to more fully understand their position in the USAF organizational structure and the continued need for professional development to be effective NCOs.[4]

Table 11 - Airman Leadership School (Appreciate)

Area	**Concepts (Appreciate)**
Nature & characteristics of the domain	• Cyberspace domain is an operational domain consisting of the entire electromagnetic spectrum (EMS) and electronic systems • Comparison / contrast with other domains of air, land, space, and sea

	• Cyberspace domain transcends all other domains
Capabilities	• The AF has a broad range of capabilities that operate in cyberspace, such as network capabilities and electronic warfare • Capabilities include offense, defense, and support • Capabilities are planned and employed in conjunction with operations in other domains to achieve national security objectives
Functions	• AF functions are performed to achieve effects in support of national security objectives • Strategic attack, cyberspace control, cyberspace interdiction, etc. • Functions include Intelligence, Surveillance and Reconnaissance, Information Operations, Command and Control, etc.
Integration & interrelationships	• Interrelationship between air, space and cyberspace forces is complex • Cyberspace capabilities can support & enhance activities in other domains • Activities in other domains can support & enhance cyberspace operations • Integrating these forces at the operational level is complex • Distinguish between cyberspace and information operations—AF position is that cyber is **not** just a rehash of IO • Military Services' primary roles, missions and organizations. This should already exist at a conceptual level. Cyber should be addressed as a third mission area for the USAF, and content will discuss at a conceptual level how cyber forces are organized, trained and equipped for cyber operations. Also describe how these forces are presented to the combatant commanders
Employment of cyber power	• Organizing for effective employment of cyber power • Primary missions and responsibilities of the combatant commands • Instruments of national power – cyberspace increasing the importance of information • Effective application of air, space and cyber-power: compress kill chain, secure C2, cross-domain dominance) • Tenets / principles of air, space, and cyber power • 24 x 7 x 365 cyber effects at all levels of war
Law, policy &	• There are restrictions on what military forces can do,

ethics	especially in the homeland (Posse Comitatus, Intelligent Oversight, Title 10/50) • Law of Armed Conflict (jus ad bellum, jus in bello, principles of discrimination & proportionality, targeting, combatants)

13. NCO Academy (NCOA):
    13.1. The NCOA broadens the leadership and management skills of TSgts and TSgt selectees. It provides more in-depth instruction than that received in ALS. The NCOA is a course of approximately 6 weeks that covers Air Force history, Air Force organization and mission, the military justice system, professional skills, customs and courtesies, leadership and management, the substance abuse program, counseling techniques, human behavior, and orientation of newly assigned personnel. The course also includes formal and informal group leadership, management theory, personnel management, problem-solving techniques, the supervisor's role in effective communication, and effective writing in the Air Force.[5]
        13.1.1. Mission: *Prepare technical sergeants to be professional, warfighting Airmen who can manage and lead Air Force units in the employment of air, space, and **cyberspace** power.*[4]
        13.1.2. Goal: Furnish an environment for students to gain an understanding of their positions in the military structure and develop the skills necessary for effectiveness in those supervisory positions.[4]

Table 12 - NCO (Knowledge)

Area	**Concepts (Knowledge)**
Nature & characteristics of the domain	• Definition of a "military domain of operations" • Cyberspace as an operational domain—i.e., a place where we conduct operations to achieve effects and exert will over the adversary • Compare / contrast with other domains of air, land, space, and sea • Cyberspace domain is an operational area consisting of the entire electromagnetic spectrum (EMS), networks, and electronic systems • Characteristics, physics, boundaries, etc. • Cyberspace domain transcends all other domains • Know the organization for national security and how defense organizations fit into the overall structure (Modification)
Capabilities	• The AF has a broad range of capabilities that operate in cyberspace, such as network capabilities and electronic warfare

	• Capabilities include offense, defense, and support • Capabilities are planned and employed in conjunction with operations in other domains to achieve national security objectives • Understand fundamentals of information operations. The Air Force position is that *cyber operations* is not just a new term for information operations. Cyberspace is a domain of operations in which we achieve effects. Information operations may be performed in all of the domains to include cyberspace. With this in mind, we will need to modify our curriculum to distinguish cyberspace as a domain for information operations to be conducted in.
Functions	• AF functions (Intelligence, Surveillance and Reconnaissance, Information Operations, Command and Control, etc.) are performed to achieve effects in support of national security objectives • Strategic attack, cyberspace control, cyberspace interdiction, etc. • Students will know how the functions support, integrate with, and depend on other functions
Integration & interrelationships	• Cyberspace capabilities can support & enhance activities in other domains • Activities in other domains can support & enhance cyberspace operations • Cyberspace is crucial to effectiveness in other domains • Integrating these forces at the operational level is complex • Distinguish between cyberspace and information operations—AF position is that cyber is **not** just a rehash of IO • Interrelationship between air, space, and cyberspace forces is complex. • Examples: jamming adversary communication and radar systems to support air, ground, and sea operations; using kinetic weapons to achieve cyber effects
Employment of cyber power	• Primary missions and responsibilities of the combatant commands • Organizing for effective employment of cyber power • Know the effects that can be achieved with information operations and the implications for tactical operations. • Instruments of national power – cyberspace increasing the importance of information • Effective application of air, space and cyber-power:

	compress kill chain, secure C2, cross-domain dominance) • Tenets / principles of air, space, and cyberspace • 24 x 7 x 365 cyber effects at all levels of war • Know that first priority is to control / dominate all three domains—whoever controls cyberspace generally controls the air, the land, the sea, and space • Military Services' primary roles, missions, and organizations. This should already exist at a conceptual level. Cyber should be addressed as a third mission area for the USAF, and content will discuss at a conceptual level how cyber forces are organized, trained and equipped for cyber operations. Also, describe how these forces are presented to the combatant commanders • Know the capabilities of other Services' weapon systems pertinent to the Service host-school systems and the synergistic effect gained from effective use of their joint capabilities
Law, policy & ethics	• Recognize how factors such as geopolitics, culture, and religion play in shaping planning and execution of joint force operations. Understand the impact of cyberspace and international communications infrastructure. • US laws (criminal, administrative, and civil) • Restrictions on what military forces can do, especially in the homeland (Posse Comitatus, Intelligent Oversight, Title 10/50) • Rules of Engagement (ROE) and tailored response options • International Laws affecting electronic communications • Military Law (UCMJ, Nat'l Security Act, Foreign Intel Surveillance Act, etc.) • Law of Armed Conflict (jus ad bellum, jus in bello, principles of discrimination & proportionality, targeting, combatants) • Understand cyberspace's use as a potential WMD/E

14. Senior NCO Academy (SNCOA)

14.1. The SNCOA is the highest level of PME available to NCOs. This 7-week resident course is conducted at Maxwell AFB/Gunter Annex, Alabama. Each year, HQ AFPC identifies CMSgt selectees, SMSgts, SMSgt selectees, and a certain number of MSgts to attend the SNCOA. This course provides the education necessary for senior NCOs to become more effective leaders and managers during peacetime, time of crisis, and conflict. SNCOA graduates

should approach their assignments with an expanded perspective of the military profession and broadened leadership and managerial capabilities. The SNCOA curriculum includes communicative skills, international relations, national objectives, employment of military force in achieving Air Force objectives, the Air Force role in force application, management, and effective use of human resources. This course also includes the individual and work environment, management concepts and theories, analytical problem solving, managerial styles, and methods of improving workers' performance. The curriculum is also designed to take the theories of sound leadership and management principles and intertwine them with QAF principles and concepts. The students are then allowed to apply these sound quality ideas to simulated case studies in making improvements within their organizations.[5]

14.1.1. Mission: Prepare senior noncommissioned officers to lead the enlisted force in the employment of air, space, and **cyberspace** power in support of our national security objectives.[4]

14.1.2. Goal: Conduct a relevant and rigorous educational program contributing to the professional development and motivation of senior NCOs.[4]

Table 13 – SNCO (Comprehension)

Area	**Concepts (Knowledge/Comprehension)**
Nature & characteristics of the domain	• Definition of a "military domain of operations" • Cyberspace as an operational domain—i.e., a place where we conduct operations to achieve effects and exert will over the adversary • Compare / contrast with other domains of air, land, space, and sea • Cyberspace domain is an operational area consisting of the entire electromagnetic spectrum (EMS), networks, and electronic systems • Characteristics, physics, boundaries, etc. • Cyberspace domain transcends all other domains • Know the organization for national security and how defense organizations fit into the overall structure (Modification)
Capabilities	• The AF has a broad range of capabilities that operate in cyberspace, such as network capabilities and electronic warfare • Capabilities include offense, defense, and support • Capabilities are planned and employed in conjunction with operations in other domains to achieve national security objectives • Understand fundamentals of information operations. The Air Force position is that *cyber operations* is not just a new term for information operations.

	Cyberspace is a domain of operations in which we achieve effects. Information operations may be performed in all of the domains to include cyberspace; With this in mind, we will need to modify our curriculum to distinguish cyberspace as a domain for information operations to be conducted in
Functions	• AF functions (e.g. Intelligence, Surveillance and Reconnaissance, Information Operations, Command and Control, etc.) are performed to achieve effects in support of national security objectives • Strategic attack, cyberspace control, cyberspace interdiction, etc. • Students will know how the functions support, integrate with, and depend on other functions
Integration & interrelationships	• Cyberspace capabilities can support & enhance activities in other domains • Activities in other domains can support & enhance cyberspace operations • Cyberspace is crucial to effectiveness in other domains • Integrating these forces at the operational level is complex • Distinguish between cyberspace and information operations—AF position is that cyber is **not** just a rehash of IO • Interrelationship between air, space, and cyberspace forces is complex • Examples: jamming adversary communication and radar systems to support air, ground, and sea operations; using kinetic weapons to achieve cyber effects
Employment of cyber power	• Primary missions and responsibilities of the combatant commands • Organizing for effective employment of cyber power • Know the effects that can be achieved with information operations and the implications for tactical operations. • Instruments of national power – cyberspace increasing the importance of information • Effective application of air, space and cyberspace: compress kill chain, secure C2, cross-domain dominance~~)~~ • Tenets / principles of air, space, and cyberspace • 24 x 7 x 365 cyber effects at all levels of war • Know that first priority is to control / dominate all three domains—whoever controls cyberspace generally controls the air, the land, the sea, and space

	• Military Services' primary roles, missions, and organizations: This should already exist at a conceptual level. Cyber should be addressed as a third mission area for the USAF, and content will discuss at a conceptual level how cyber forces are organized, trained and equipped for cyber operations. Also, describe how these forces are presented to the combatant commanders • Know the capabilities of other Services' weapon systems pertinent to the Service host-school systems and the synergistic effect gained from effective use of their joint capabilities
Law, policy & ethics	• Recognize how factors such as geopolitics, culture, and religion play in shaping planning and execution of joint force operations. Understand the impact of cyberspace and international communications infrastructure • US laws (criminal, administrative, and civil) • Restrictions on what military forces can do, especially in the homeland (Posse Comitatus, Intelligent Oversight, Title 10/50) • Rules of Engagement (ROE) and tailored response options • International Laws affecting electronic communications • Military Law (UCMJ, Nat'l Security Act, Foreign Intel Surveillance Act, etc.) • Law of Armed Conflict (jus ad bellum, jus in bello, principles of discrimination & proportionality, targeting, combatants) • Cyberspace's use as a potential WMD/E

Possible Additional Content / Material

- Cyber's impact on the art of warfare (i.e. effects of information revolution on warfare)[6]
- Managing information overload –finding the critical information[7]
- Emerging technologies[7]
- Adaptability/agility/people focus over thing focus
- Need for warrior-scholar[8]
- Strategic communication[9]
- Information age – broadened threat context[10]
- Low entry cost, blurring traditional boundaries, strategic intelligence, perception management, tactical warning and attack assessment, building and sustaining coalitions, and vulnerability of US homeland[11]

- Appreciating cyberspace as a COG for US
- Application of principles of war is the same in cyberspace
- Coordination of military (DoD) and commercial efforts – DHS, CIA, NSA, DIA, FBI, etc. all have irons in this fire
- Considering that the curricula are so full in all PME environments, emphasis should be taken to decrease the material that is repeated. For example, the same exact things that show up in ASBC, SOS, and ACSC can be thinned out to make room for the critical subject of cyberspace.
- It also seems that the IO/IW curricula will have to change. Since some of IO will be covered in cyberspace objectives, additional "room" can be made there. Cyberspace is now part of the AF mission statement. PME has made it a part of most of their missions, and therefore, the material must make it into the curriculum.

References

1. Concept of Cyber Warfare. Eighth Air Force, United States Air Force. 1 June 2007.

2. Information Operations: Air Force Doctrine Document 2-5. United States Air Force. 11 January 2005.

3. Air Force Instruction 36-2301: Professional Military Education. United States Air Force. 27 June 2002.

4. Air University Catalog 2006-2007. Air University Press. Maxwell Air Force Base, Alabama. July 2006 .

5. "Enlisted Professional Military Education." 9 Sep 2004 http://fromtheinside.us/mentor/guideafondod-part7.htm.

6. Wynne, Michael W. "Cyberspace as a Domain In which the Air Force Flies and Fights." 2 Nov 2006. http://www.af.mil/library/speeches/speech.asp?id=283.

7. "Developing the Warrior-Scholar." Maj Scott Efflandt. *Military Review*. July-August 2001.

8. Joint Chiefs of Staff. "2007 JPME Special Areas of Emphasis." 15 Feb 2007

9. Pattillo, Lt Col Chuck. "Education for Transformation." March 2004.

10. Molander, Roger. Riddile, Andrew. Wilson, Peter. Strategic Information Warfare – A New Face of War. National Defense Research Institute. Santa Monica, CA. 1996.

11. Leadership and Force Development: Air Force Doctrine Document 1-1. United States Air Force. 18 February 2006.

12. Berg, Lt Col Paul. "Air Force Cyber Command: What It Will Do and Why We Need It." *Air & Space Power Journal*. 20 February 2007. http://www.airpower.au.af.mil/apjinternational/apj-s/2007/1tri07/bergeng.html

13. Chairman of the Joint Chiefs of Staff Instruction 1800.01C: Officer Professional Military Education Policy (OPMEP). CJCS. 22 December 2005.

14. Chairman of the Joint Chiefs of Staff Instruction 1805.01: Enlisted Professional Military Education Policy (EPMEP). CJCS. 28 October 2005.

15. General Defense Intelligence Program: Information Technology Strategic Plan 2008-2013. Defense Intelligence Agency. Washington, DC. April 2006.

16. "FBI Information Strategic Plan Synopsis." Federal Bureau of Investigation. November 2004.

17. "Information Operations Primer." US Army War College, November 2006. AY 2007 Edition.

18. Information Operations: Joint Publication 3-13. Joint Chiefs of Staff. 13 February 2006.

19. "Workforce Preparation, Education, and Research Working Group." National Infrastructure Advisory Council. 11 April 2006.

20. Henderson, MSgt Terence D. "USAF Enlisted Professional Military Education." *Air & Space Power Journal*. 2005

Cyber PME Community of Interest

Name	Unit
Maj Susan Airola-Skully	AF/A1DL
LtCol Jeffrey Boleng	USAFA
Ctr Thomas Bullard	ACC/A3I
Ctr Ina Downey	AF/A3O-CP
LtCol David Fahrenkrug	8AF
Maj Timothy Franz	8AF
Col David (Hoot) Gibson	USAFA
LtCol John Glock	ACSC/DLC
LtCol Paula Gregory	SAF/XCI
LtCol Forrest Hare	AF/Cyber Task Force
Dr Kamal Jabbour	AFRL/IF
Maj Rose Jourdan	AF/A1DO
LtCol Michael Linschoten	ACSC/DEP
Col Stephen McPherson	AF/Cyber Task Force
Dr Robert Mills	AFIT/ENG
Civ Roger Philipsek	AFDC/WE
LtCol Scott Poynter	NGB/A2
Dr Richard Raines	AFIT/ENG
Dr Thomas Renckly	AU/CFA
Capt Jeffrey Scohy	AFROTC/DOTT
Col James Smith	AWC/DFJ
LtCol Bertrand Sparrow	ACSC/DEI
Civ George Stein	AWC/DFJ
Maj Joseph Trechter	SAF/XCI
Ctr Daffney Walker	AF/A3O-CP
Maj Paul Williams	AFIT/ENG
LtCol Clifford (Doug) Williams	SOC
Col Stephen (Wilbur) Wright	AWC/DF